Mitigation of cybersecurity risks in production facilities

A complete overview of vulnerabilities in its production facilities helped a worldwide chemical company to mitigate cybersecurity risks. CGI provided a team of OT cybersecurity experts to assess the production facilities.

As the client started an Operational Technology (OT) cybersecurity program, the purpose of this program was to prevent:

- Safety incidents from occurring as the result of cybersecurity events
- Production discontinuities, plant disasters, ransomware attacks, etc.
- Loss of intellectual property, product quality, and reputation damage

The challenge

Most companies often don't have all of the expert knowledge and capacity readily available to address cybersecurity threats effectively. One of our clients needed specific expert insights and more of an overview of all cybersecurity risks and mitigation of all threats and vulnerabilities in its factories. This included all operational technology computing systems that are used to manage the entire industrial operation. Industrial control systems (ICS) typically in place comprise systems such as Manufacturing Execution Systems (MES), Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) Programmable Logic Controllers (PLCs), and Safety Instrumented Systems (SIS). These systems are used to monitor and control industrial processes. ICSs are typically mission-critical applications with a high-availability requirement.

The solution

CGI was selected to execute assessments based on the long trusted security partnership between the two companies. A team of CGI' OT cybersecurity experts assessed the factories, against the client' OT cybersecurity standards & practices, with the client itself assigning each of the sites a specific complexity level, low, medium or high. A classification based on the number of systems under consideration, the local available expertise and the criticality of the site for the client.

For each of these classifications, a uniform, but tailored approach was created by CGI to perform the assessments.

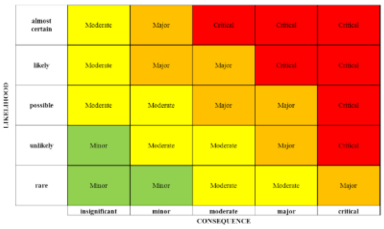
OT / ICS CYBERSECURITY ASSESSMENTS INCLUDE

- Planning
- Data collection
- Site visits
- Reporting
- Remediation advice

Prior to the site visits, sites were supported by a CGI assessment preparation team to ensure that all required information, such as network diagrams and asset inventory, to conduct the assessment were available at the time of the assessment.

CGI executed the assessments with multiple on-site assessor teams specialized in OT security. The assessments included structured interviews with key employees, physical security, analysis and assessment of the OT / ICS network, the connected OT systems and the processes for anti-malware, identity & access management, firewalls and remote access.

The assessments provided a clear insight in the maturity of the OT security policy in place as well as the way in which this policy was implemented, and measures to be taken in regards to any gaps.



LIKELIHOOD	almost certain	Moderate	Major	Critical	Critical	Critical
	likely	Moderate	Major	Major	Critical	Critical
	possible	Moderate	Moderate	Major	Major	Critical
	unlikely	Minor	Moderate	Moderate	Major	Critical
	rare	Minor	Minor	Moderate	Moderate	Major
		insignificant	minor	moderate	major	critical

CONSEQUENCE

The Assessment report included a Business Impact Assessment for every system under consideration, a Risk Assessment and a Compliance Tracker, with specific mitigation advice for every observation.

The risk assessment, covering risks, likelihood and business impact, recommended mitigations were pre-prioritized and helped the client to define its OT / ICS cybersecurity priorities moving forward.

Why CGI

Clients choose CGI for its capability in mission critical environments and OT cybersecurity with the capacity and ability to assess factories and business operations worldwide, with a uniform approach and within an agreed time frame. CGI is able to provide a team of experts with deep knowledge in the process control domain.

About CGI in cybersecurity

CGI has over 40 years of heritage in creating and securing critical business systems in complex, environments across the globe, including defense and intelligence sectors.

We have invested in establishing our credentials, working closely with international security associations and standards bodies. While cyber threats are global, we know that requirements vary locally and challenges are unique to each organization. Through our expert talent, deep technical and business knowledge, security operations centers, best practices and frameworks, we work to ensure controls are baked in, not bolted on.

> “…the manufacturing industry is one of the most vulnerable and targeted industries when it comes to cyberattacks”

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 76,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cginederland.nl
Email us at info.nl@cgi.com